

ABSTRACT

A method is provided for use in the secured transmission of information in a networked environment. Network communications are bi-directionally enabled and encrypted. The need or ability for any individual to access an account encryption Key is eliminated and only communication devices have access to an operational account Key

5 that is used to encrypt or decrypt data passing through the device. A master Key is established and stored at a Recipient Device. Messages that are sent to the Recipient Device may optionally include an intermediate Key exclusive to that message. A method of integrating security hardware to protect the integrity of account data and Keys is also provided. Hardware or software tampering is also monitored. A method of sending the

10 Key to a device in an encrypted form during registration is also provided. A method to perform all encryption and decryption without impeding the data communication rate is provided.